

Exam : NSE4_FGT-7.2

Title : Fortinet NSE 4 - FortiOS 7.2

https://www.passcert.com/NSE4_FGT-7.2.html

1. Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srcintfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because Action is set to DENY in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to error on FortiGate.

Answer: A,C

2. Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: A,C

3. Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
  pingsvr_flip_timeout/expire=3600s/2781s
  'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
  'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

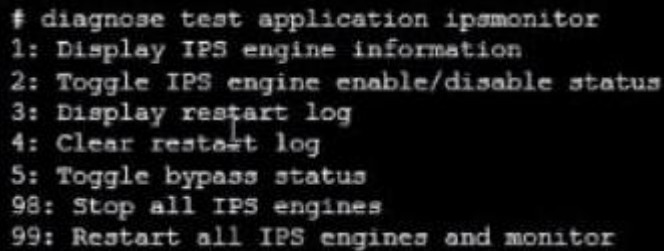
Answer: A,D

Explanation:

1. Override is disabled by default - OK
2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary" The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab>

4.Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: A

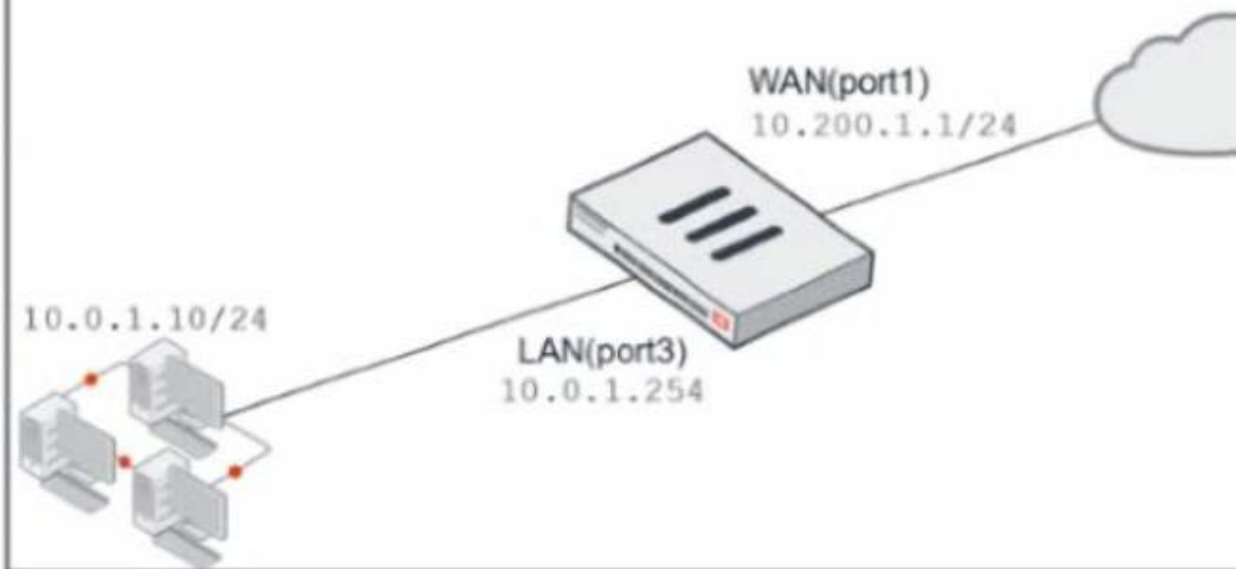
Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage>

5.Refer to the exhibit.

Network diagram



Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 6/255
Color	Change

IP Pool

Name
Comment
Type
External IP

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration.

The WAN (port1) interface has the IP address 10.200. 1. 1/24.

The LAN (port3) interface has the IP address 10 .0.1.254. /24.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1
- B. 10.200.3.1
- C. 10.200.1.100
- D. 10.200.1.10

Answer: C

Explanation:

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

6. In which two ways can RPF checking be disabled? (Choose two)

- A. Enable anti-replay in firewall policy.
- B. Disable the RPF check at the FortiGate interface level for the source check
- C. Enable asymmetric routing.
- D. Disable strict-arc-check under system settings.

Answer: C,D

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

7. Refer to the exhibit.

The screenshot shows the configuration for SLA_1. The Name is SLA_1. The Protocol is Ping. The Servers are 4.2.2.2 and 4.2.2.1. The Participants are All SD-WAN Members, with a Specify button. Below this, there is a list of participants: port1 and port2. At the bottom, there is a checkbox for 'Enable probe packets' which is currently unchecked.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.

Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

Answer: B,D

8. Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The common name on the subject field must use a wildcard name.
- C. The issuer must be a public CA.
- D. The CA extension must be set to TRUE.

Answer: A,D

Explanation:

"In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign."

Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

9.Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

Answer: D

Explanation:

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

10.What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: B

11.A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service. What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

Answer: B

Explanation:

Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup client and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

12.Examine this PAC file configuration.

Which of the following statements are true? (Choose two.)

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: A,D

13.Refer to the exhibits.

Exhibit A

The screenshot shows the 'Edit Policy' window for a policy named 'Facebook SSL Inspection'. The configuration is as follows:

Field	Value
Name	Facebook SSL Inspection
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL

Below the policy settings, there is a section for 'Firewall / Network Options' with a message: 'Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.'

The 'Security Profiles' section shows 'SSL Inspection' is enabled and set to 'certificate-inspection'.

Exhibit B

The screenshot shows the 'Edit Policy' window for a policy named 'Facebook Access'. The configuration is as follows:

Field	Value
Name	Facebook Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	App Default
Application	Facebook, Facebook_Like.Button, Facebook_Video.Play
URL Category	+
Action	ACCEPT

Below the policy settings, there is a section for 'Firewall / Network Options' with 'Protocol Options' set to 'default'.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. Make SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Get the additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

Answer: A

Explanation:

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather than adding an app rule.

14.View the exhibit.

The exhibit shows two static route configurations on a FortiGate device. Both routes are for the destination 172.13.24.0/255.255.255.0.

- Left Screenshot (TunnelB):**
 - Destination: Subnet (172.13.24.0/255.255.255.0)
 - Interface: TunnelB
 - Administrative Distance: 5
 - Status: Enabled
 - Priority: 30
- Right Screenshot (TunnelA):**
 - Destination: Subnet (172.13.24.0/255.255.255.0)
 - Interface: TunnelA
 - Administrative Distance: 10
 - Status: Enabled
 - Priority: 0

Which of the following statements are correct? (Choose two.)

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
- D. This is a redundant IPsec setup.

Answer: C,D

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundancy>

15.Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

Answer: A,D

Explanation:

Reference:

https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

16.Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Answer: C,D

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

17.Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

18.An administrator is running the following sniffer command:

Which three pieces of Information will be Included in me sniffer output? {Choose three.}

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

Answer: A,B,D

19.An administrator does not want to report the logon events of service accounts to FortiGate.

What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add user accounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

Answer: D

Explanation:

Reference:

<https://community.fortinet.com/t5/Support-Forum/Collector-Agent-and-problem-getting-login-info/m-p/95481>

20.Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

21.Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: B,C,E

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview>